OIPE JC177
MAR 05 2004
PATENT & TRADEMARK OFFICE

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Ivan Laloux SBIDA

Group Art Unit: 2631

Application No.: 10/677,751

Examiner: Unassigned

Filed: October 3, 2003

Attorney Dkt. No.: 60282.00103

For: METHOD, SYSTEM AND NETWORK ELEMENT FOR DATA TRANSMISSION USING A TRANSITION MECHANISM

CLAIM FOR PRIORITY UNDER 35 USC § 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

March 5, 2004

Sir:

The benefit of the filing dates of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

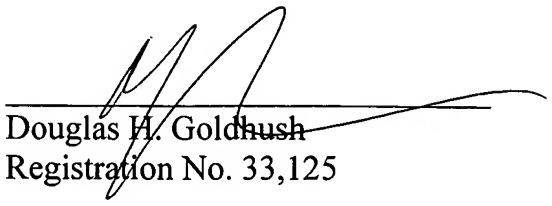
European Application No. 03014728.4 filed on June 27, 2003 in Europe

In support of this claim, certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Counsel's Deposit Account No. 50-2222.

Respectfully submitted,



Douglas H. Goldhush
Registration No. 33,125

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DHG:lls

Enclosure: Priority Document (1)

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the European patent application described on the following page, as originally filed.	Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr.	Patent application No.	Demande de brevet n°
	03014728.4	

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03014728.4
Demande no:

Anmeldetag:
Date of filing: 27.06.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Nokia Corporation
Keilalahdentie 4
02150 Espoo
FINLANDE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method, system and network element for data transmission using a transition mechanism

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L12/56

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

TBK TIEDTKE - BÜHLING - KINNE & PARTNER (GbR)

TBK-Patent POB 20 19 18 80019 München

Patentanwälte
Dipl.-Ing. Reinhard Kinne
Dipl.-Ing. Hans-Bernd Pellmann
Dipl.-Ing. Klaus Grams
Dipl.-Ing. Aurel Vollnhals
Dipl.-Ing. Thomas J.A. Leson
Dipl.-Ing. Dr. Georgi Chivarov
Dipl.-Ing. Matthias Grill
Dipl.-Ing. Alexander Kühn
Dipl.-Ing. Rainer Böckelen
Dipl.-Ing. Stefan Klingele
Dipl.-Chem. Stefan Bühling
Dipl.-Ing. Ronald Roth
Dipl.-Ing. Jürgen Faller
Dipl.-Ing. Hans Ludwig Trösch
Rechtsanwälte
Michael Zöbisch

EPO - Munich
3
27. Juni 2003

US.38387
July 27, 2003

NOKIA CORPORATION
Espoo, Finland

METHOD, SYSTEM AND NETWORK ELEMENT FOR DATA TRANSMISSION USING A TRANSITION MECHANISM

Dresdner Bank München Kto. 3939 844 BLZ 700 800 00
Deutsche Bank München Kto. 286 1060 BLZ 700 700 10
Postbank München Kto. 67043 804 BLZ 700 100 80
Mizuho Corp. Bank Düsseldorf Kto. 8104233007 BLZ 300 207 00
UFJ Bank Limited Düsseldorf Kto. 500 047 BLZ 301 307 00
/RS218

Telefon: +49 89 544690
Telefax (G3): +49 89 532611
Telefax (G3+G4): +49 89 5329095
E-Mail: postoffice@tbk-patent.de
Internet: http://www.tbk-patent.de
Bavariaring 4-6, 80336 München

METHOD, SYSTEM AND NETWORK ELEMENT FOR DATA TRANSMISSION USING A TRANSITION MECHANISM

BACKGROUND OF THE INVENTION

Field of the invention

The present invention relates to a method and/or a system and/or a network node usable for controlling a data transmission in a communication network. In particular, the present invention is related to a data transmission control in a communication network which uses different types of transmission mechanisms or protocols, such as for example IPv4 and IPv6, particularly in a coexistence phase during a transition from one transmission mechanism to another (new) transmission mechanism in the communication network.

Related prior art

In the last years, an increasingly extension of data and communication networks, i.e. of wire based networks, such as the Integrated Services Digital Network (ISDN), or wireless networks, such as the cdma2000 (code division multiple access) system, Universal Mobile Telecommunications System (UMTS), the General Packet Radio System (GPRS), or other wireless communication system, such as the Wireless Local Area Network (WLAN), took place all over the world. Various organizations, such as the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), 3rd Generation Partnership Project 2 (3GPP2), Internet Engineering Task Force (IETF), and the like are working on standardization for such networks.

In general, the system structure of a communication network is such that a user equipment, such as a mobile station, a mobile phone, a fixed phone, a personal computer (PC), a laptop, a personal digital assistant (PDA) or the like, is connected via transceivers and interfaces, such as an air interface, a wired interface or the like, to an access network subsystem. The access network subsystem controls the communication connection to and from the user equipment and is connected via an interface to a corresponding core or backbone network subsystem. The core (or backbone) network subsystem switches the data transmitted via the communication connection to a destination, such as another user equipment, a service provider (server/proxy), or another communication network. The core network subsystem may be connected to a plurality of access network subsystems. The respective network structure may vary, as known for those skilled in the art and defined in respective specifications, for example, for UMTS, GSM and the like.

Generally, for properly establishing and handling a communication connection between network elements such as the user equipment and another user terminal, a database, a server, etc., one or more intermediate network elements such as support nodes or service nodes are involved. Data, such as voice, multimedia, control signaling data and the like, are transmitted, for example, by means of a packet based data transmission. One example for a utilized packet based data transmission protocol is the Internet Protocol (IP). For this protocol type, there are currently available several versions, for example, IPv4, and the like, which are commonly known. However, due to changing requirements and load conditions in the networks, more sophisticated versions have been developed, such as IPv6.

For example, with regard to the above mentioned IPv4 and IPv6, the IPv4 address space is being rapidly exhausted as new nodes and networks are added to Internet routing structure. One great benefit of IPv6 is that it provides a considerably larger address space. Although addressing capabilities of IPv4 have been successfully extended by introducing, for example, private addressing, temporary global addresses and address translators, it can be foreseen that with the current growth rate of the Internet, in terms of number of hosts connected to it and in terms of adoption of new services, the number of unique globally routable addresses being available in IPv4 addressing domain is not sufficient for the future needs. Thus, one main motivation for IPv6 deployment results from the need for global reachability of Internet hosts. Furthermore, IPv6 offers also an enhanced security level and mobility support.

Of course, when network operators change the existing IPv4 network environment to IPv6, there will be a transition period when IPv4 hosts coexist with IPv6 hosts. Taking this into consideration, there have been developed several transition mechanisms which aim to maintain interoperability during this transition period between IPv4 and IPv6 parts. These mechanisms can generally be classified into three main groups: Dual Stack, Tunneling and Protocol Translation. A Dual Stack node implements both IPv4 and IPv6 protocol stacks, allowing connection to both IPv4 and IPv6 networks. Tunneling is a forwarding technique in which a packet is encapsulated into another type of packet, i.e. IPv6 datagrams are encapsulated within IPv4 packets and decapsulated at a corresponding receiving node, for example. Thus, this technique provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic, or vice versa. Tunneling requires dual stack

functionality in both encapsulating and decapsulating nodes. Finally, Protocol Translators are required when two communicating nodes are not sharing the same version of IP.

In "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" by F. Templin et al. (see also Internet draft *draft-ietf-ngtrans-isatap-13.txt*), there is defined one example of a specific type of such an transition mechanism for providing IPv6 connectivity within an IPv4 network. Another example for a transition mechanism is disclosed, for example, in RFC (Request for Comments) 3056, "Connection of IPv6 Domains via IPv4 Clouds" by B. Carpenter et al.

As shown in Fig. 5, in case of ISATAP, ISATAP nodes have special IPv6 addresses with a special ISATAP format interface identifier, which embeds an IPv4 address. The ISATAP address format comprises two portions, i.e. a network portion (IPv6 prefix) and a host portion. ISATAP nodes are assigned a normal IPv6 prefix 11 (i.e. 64-bit size) which can be link-local, site-local or global scope, and the specific ISATAP format interface identifier 12, 13 (i.e. 32 + 32 bit = 64-bit size). The interface identifier is constructed by using a "modified EUI-64" format according to IEEE EUI-64 standard by appending an IPv4 address 13 (which is assigned to the node) to a 32-bit string '00-00-5E-FE' (reference sign 12) which comprises an organizationally-unique identifier (OUI) and a respective type field. For the IPv4 address either public or private IPv4 addresses can be used.

In Fig. 6, an example for an implementation of a transition mechanism, such as ISATAP, in a communication network, for example a 3GPP based communication network, is shown.

According to Fig. 6, reference sign 5 denotes a user equipment (UE) which is a dual stack device implementing both IPv4 and IPv6 stacks. Reference sign 21 denotes a Gateway GPRS Support Node (GGSN) representing a control network element of a 2G/3G mobile network 30. As commonly known, the 2G/3G mobile network further comprises access network subsystem elements and core network subsystem elements (not shown) for establishing and controlling a communication connection of the UE 5. Reference sign 100 denotes a IPv4 based operator network. Reference sign 40 denotes an operator services portion of the operator network which comprises one or more IPv6 based application servers (only one thereof is shown) providing IPv6 based services. Reference sign 50 denotes an IP Multimedia Subsystem comprising a Proxy Call State Control Function (P-CSCF), an Interrogating Call State Control Function (I-CSCF), and a Serving Call State Control Function (S-CSCF). Reference sign 60 denotes an edge or border router. The above mentioned elements are known to a person skilled in the art so that a detailed description thereof can be omitted.

According to ISATAP, the site's IPv4 infrastructure 100 is treated as a link layer for IPv6 communications using automatic IPv6-in-IPv4 tunneling. This enables an incremental deployment of IPv6 infrastructure within the IPv4 sites with no scaling issues at border gateways. Moreover, no special IPv4 services within the site (e.g., multicast) are required. In addition, ISATAP supports both manual address configuration and stateless address autoconfiguration, and it is compatible with other transition mechanisms, e.g., the 6to4 tunneling according to RFC 3056.

As also shown in Fig. 6, ISATAP nodes are dual stack terminals 5 which are capable of automatically tunneling data packets to the IPv6 next-hop address through the IPv4 infrastructure. This means that for the application of the ISATAP mechanism in a 3GPP network the ISATAP functionality (i.e. packet encapsulation/decapsulation, etc.) resides in the UE 5. Thus, in the example shown in Fig. 6, the IPv6-in-IPv4 tunneling is performed in the UE 5. Packets are sent via the 2G/3G mobile network's GGSN 21 by means of IPv4 PDP context connection 6, and the corresponding ISATAP links 46 and 56 extend from the UE 5 to the respective IPv6 service located in portions 40 and/or 50.

However, the usage of a transition mechanism, such as ISATAP, may increase the complexity of the communication system and, for example, the costs of a corresponding user equipment. When deploying, for example, ISATAP in a 3GPP cellular operator network, the UEs must implement all the ISATAP node functionality in order to allow tunneling of IPv6 packets over the IPv4 network (i.e., encapsulation/decapsulation is performed in the UE). This involves a huge increase in the complexity and costs of the UEs, and different vendors have to implement ISATAP in their terminals in order to enable IPv6 connections within an IPv4 operator network. Therefore, the deployment of transition mechanism, and thus also of more sophisticated communication protocols or the like in an existing network structure, may become complicated, and there is the possibility that the migration to the more sophisticated communication technique, e.g. the migration from IPv4 to IPv6, is decelerated since a demand of IPv6 services by the vast majority of users is reduced because presumably only high-end (and expensive) terminals are capable of accessing IPv6 services.

SUMMARY OF THE INVENTION

Thus, it is desirable to provide an improved mechanism for controlling a data transmission in connection with a transition mechanism which allows to overcome the above limitations.

This is achieved by the measures defined in the appended claims.

According to one aspect of the proposed solution, there is provided, for example, a method of controlling a data transmission from a first node to a second node via a communication network wherein the first node is connected to the communication network by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node, the method comprising the steps of activating a communication connection based on the communication protocol of the first type from the first node to a network node of the communication network, allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, allocating, based on a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, and storing, by the network node, the first connection information part and the second connection information part in a register, wherein the second connection information part is associated with the first connection information part in a common entry in the register.

Furthermore, according to one aspect of the proposed solution, there is provided, for example, a system for controlling a data transmission from a first node to a second node via a communication network the first node is connected to the communication network by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node the system comprising means for activating a communication connection based on the communication protocol of the first type between the first node and a network node of the communication network, means for allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, means for allocating, on the basis of a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, and means for associating the second connection information part with the first connection information part and for storing the associated first and second connection information parts in a register.

Moreover, according to one aspect of the proposed solution, there is provided, for example, a network node of a communication network, the network node being usable for controlling a data transmission from a first node to a second node via the communication network wherein the first node is connected to the network node by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node, the network node comprising means for activating a

communication connection based on the communication protocol of the first type between the first node and the network node, means for allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, means for allocating, on the basis of a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, and means for associating the second connection information part with the first connection information part and for storing the associated first and second connection information parts in a register.

According to further refinements, the proposed solution may comprise one or more of the following features:

- for the activation of the communication connection, an activation request may be sent from the first node to the network node, the activation request comprising at least one of an indication for a dynamic addressing and an indication of an address type for the communication protocol of the first type;

- for allocating the first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, the address related to the communication protocol of the first type may be allocated by the network element;

- for allocating the first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, the address related to the communication protocol of the first type may be requested from an external address allocation element contacted by the network element;

- for allocating the second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, the address related to the communication protocol of the second type may be allocated by the network element from an internal pool of addresses;

- for allocating the second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, the address related to the communication protocol of the second type may be requested from an external address allocation element contacted by the network element;

- the network element may store the first connection information part and the second connection information part associated with each other by an entry in a table portion related to the communication connection of first node, wherein the second connection information part may be stored in a specific table field of the table portion;

- the data transmission based on the communication protocol of the first type may be tunneled between the first node and the second node via the network node by means of a connection based on the communication protocol of the second type;

- the data transmission may be a packet based data transmission, the communication protocol of the first type may be one type of an Internet protocol, in particular an IPv6 based protocol, and the communication protocol of the second type may be another type of an Internet protocol, in particular an IPv4 based protocol;

- the communication connection between the first node and the network node may be based on a packet based data transmission protocol context, in particular on a Packet Data Protocol context;

- the transition mechanism used by the communication network may be an automatic tunneling mechanism which uses

in particular the Intra-Site Automatic Tunnel Addressing Protocol;

- the network node may be a gateway node of the communication network, in particular a Gateway GPRS Support Node.

By virtue of the proposed solutions, the following advantages can be achieved:

- It is possible that the complete functionality of the transition mechanism is centralized in a network node of the communication network and does not need to be performed in the user equipment. For example, the ISATAP functionality can be performed by a GGSN instead of the UE. For example, IPv6 tunneling over an IPv4 operator network is achieved by performing encapsulation/decapsulation of packets in the operator network. Hence, by providing a transition mechanism proxy in the communication network, e.g. an ISATAP proxy for the 3GPP network it is possible that the GGSN implements all the ISATAP functionality on behalf of the UE, thus avoiding an unnecessary increase in the terminal's (UE's) complexity and costs.

- The proposed solution can be easily implemented by means of modifications in existing network node structures, such as the GGSN. On the other hand, no additional configuration is needed in the terminals, such as the UE. Preferably, the proposed solution can be implemented by means of software modifications.

- The transition mechanism (e.g. ISATAP) functionality employed by the network node is transparent to the UE which allows the usage of terminals not specifically prepared for the transition mechanism. In particular, it is not required that the UE is a dual stack UE, i.e. it is sufficient when the UE supports, for example, the access to IPv6 services, such as IP Multimedia Subsystem (IMS) or the like. However, the invention is also applicable in connection with such dual stack terminals. Thus, almost any terminal is able to

make use of IPv6 services, which results in increasing the demand of new end-to-end services and paving the way for, e.g., IPv6 migration.

The above and still further objects, features and advantages of the invention will become more apparent upon referring to the description and the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows an example for an implementation of a transition mechanism in a communication network according to the present invention.

Fig. 2 shows an example of a packet based data transmission protocol address information element.

Fig. 3 shows a communication connection activation procedure according to one embodiment of the present invention.

Fig. 4 shows a communication connection activation procedure according to another embodiment of the present invention.

Fig. 5 shows an illustration of an ISATAP address format.

Fig. 6 shows an example for an implementation of a transition mechanism in a communication network.

DESCRIPTION OF PREFERRED EMBODIMENTS

According to the proposed solution, a data transmission from a first node, such as a subscriber's terminal node or user equipment UE, to a second node, such as an application

server or a multimedia subsystem like IMS, via a communication network, such as a 3GPP communication network, is controlled by means of a transition mechanism. This means that the communication network implements a communication protocol of a first type, such as IPv6, and at least in part a communication protocol of a second type, such as IPv4, in the operator network. The transition mechanism is located in the communication network, for example, in a gateway node like a GGSN. This means that the network node acts as a transition mechanism proxy for the data transmission. Hence, a data transmission from the first node is forwarded (or tunneled) by the network node to the second node wherein the transition mechanism functionality is performed in the network node transparently for the first node.

Here, it is to be noted that the term communication network is to be understand not only as a type of one single network but also as a network type which can be split into other network types, such as an operator's network, a radio access network, etc..

The user equipment (UE) may be a terminal apparatus of different type. For example, the UE may be a mobile or fixed phone, a personal computer, a server, a mobile laptop computer, a personal digital assistant (PDA) or the like. Irrespective of its specific type, the UE may comprise several means which are required for its communication functionality. Such means are for example a processor unit for executing instructions and processing data for the communication connection (e.g. transmission content and signaling related data), memory means for storing instructions and data, for serving as a work area of the processor and the like (e.g. ROM, RAM, EEPROM, and the like), input means for inputting data and instructions by

software (e.g. floppy diskette, CD-ROM, EEPROM, data interface means, and the like), user interface means for providing monitor and manipulation possibilities to a user (e.g. a screen, a keyboard, a microphone and headset for communication, and the like), and network interface means for establishing a communication connection under the control of the processor unit (e.g. wired or wireless interface means, an antenna, and the like). These means can be integrated within one device (e.g. in case of a mobile or fixed telephone) or in several devices forming the user equipment (e.g. in case of a laptop).

The network node used as the transition mechanism proxy, such as the GGSN, may be implemented by software or by hardware. In any case, for executing its respective functions, correspondingly used devices or network elements comprise several means which are required for control and communication functionality. Such means are, for example, a processor unit for executing instructions and processing data (for example, transmission content and signaling related data), memory means for storing instructions and data, for serving as a work area of the processor and the like (e.g. ROM, RAM, EEPROM, and the like), input means for inputting data and instructions by software (e.g. floppy diskette, CD-ROM, EEPROM, and the like), user interface means for providing monitor and manipulation possibilities to a user (e.g. a screen, a keyboard and the like), and interface means for establishing a communication connection under the control of the processor unit (e.g. wired and wireless interface means, an antenna, and the like).

In the following, a first embodiment is described with reference to Figs. 1 to 3. This first embodiment is directed to a case where IPv4 and IPv6 are implemented in

the communication network based on the 3GPP specifications, and the utilized transition mechanism is based on ISATAP.

In Fig. 1, reference sign 10 denotes a user equipment (UE). The UE 10 may be an only IPv6 capable terminal device or a dual stack device implementing both IPv4 and IPv6 stacks. Reference sign 20 denotes a Gateway GPRS Support Node (GGSN) representing a control network element of a 2G/3G mobile network 30. The GGSN 20 is a dual stack GGSN implementing both IPv4 and IPv6 stacks. It is to be noted that the 2G/3G mobile network further comprises (not shown) access network subsystem elements, such as base stations and the like, and core network subsystem elements, such as a Serving GPRS Support Node (SGSN), for establishing and controlling a communication connection to and from the UE 10. Reference sign 100 denotes a IPv4 based operator network. Reference sign 40 denotes an operator services portion of the operator network 100 which comprises one or more IPv6 based application servers (only one is shown in the figure) providing IPv6 based services. Reference sign 50 denotes an IP Multimedia Subsystem (IMS) comprising a Proxy Call State Control Function (P-CSCF), an Interrogating Call State Control Function (I-CSCF), and a Serving Call State Control Function (S-CSCF). The IPv6 application server and the IMS represent two of several possibilities for nodes providing IPv6 services which the UE 10 can access via the IPv4 operator network. Reference sign 60 denotes an edge or border router which is not essential for the proposed mechanism but is introduced so as to illustrate that the operator network 100 is connectable to other networks / resources through corresponding edge or border routers.

In the GGSN 20, the ISATAP functionality (e.g. encapsulation/decapsulation, and the like) is implemented.

On the other hand the ISATAP functionality is completely transparent to the UE 10. The UE 10 is connected to the network (i.e. to the GGSN 20) by using an IPv6 packet based data transmission protocol context, i.e. in the present example by an IPv6 PDP context based communication connection 15. Data packets are transmitted via this connection 15 and an IPv6-in-IPv4 tunneling procedure is performed in the GGSN 10. Thus, corresponding ISATAP links 45, 55 extend between the IPv6 application services (operator services 40 located or IMS 50 located) and the GGSN 20.

In the scenario according to Fig. 1, for example, an IPv6 / dual stack UE 10 attempts to access an internal IPv6 service provided by the network operator (e.g., IMS 50), while the operator network 100 is still IPv4 based, i.e. the the migration to IPv6 is not finalized.

In Fig. 3, a PDP context activation procedure is illustrated which is performed by the UE 10 in order to establish a communication connection via the mobile network 30 to the desired service (e.g. IMS 50). The PDP context activation procedure utilized in the present embodiment is based on a standard PDP Context Activation Procedure defined in 3GPP specification TS 23.060, and only those steps of the procedure relevant for the present example are described in greater detail.

If no IPv6 PDP context has been previously activated, the UE 10 requests the activation of a new IPv6 PDP context (step 1) by sending a corresponding request to the network's SGSN (not shown in Fig. 1). A PDP address information element is sent according to the standard procedure (3GPP TS 23.060) of activating a PDP context. When the UE 10 wants to establish an IP connection it has

to activate a PDP context, and such PDP context is directly related to the IP address assigned to the UE. Moreover, when following the standard procedure to activate a PDP context, the UE sends a "Activate PDP Context Request" message (3GPP TS 23.060) to the SGSN, and such message includes the PDP address information element described below.

According to the present embodiment, the Activate PDP Context Request message sent by the UE 10 specifies a dynamic IPv6 address in the PDP Address information element. Furthermore, an Access Point Name information element in the request message includes the desired access point name (APN) which corresponds to the desired internal IPv6 service (e.g. IMS 50).

An example of the PDP Address information element according to the present embodiment is shown in Fig. 2. The PDP Address information element of the Activate PDP Context Request message comprises a plurality of data octets 1 to N defining respective information portions of the PDP Address information element. These information portions comprise a packet data protocol address information element identifier (IEI), a portion defining a length of PDP address contents, a portion defining a PDP type organization, a portion defining a PDP type number, and a portion defining address information. Additionally, some portions may be spared by definition.

For the request of the UE 10 for the activation of a new (IPv6) PDP context in order to access an IPv6 internal service, the content of the PDP Address information element of the Activate PDP Context Request follows one or more of the rules defined below in order to force the allocation of a dynamic IPv6 address:

- the value of octet 2 is 0000 0010 (indicating dynamic IP addressing);
- the value of octet 3 (PDP type organisation field) is 0001 (IETF allocated address);
- the value of octet 4 is 01010111 (IPv6 address);
- the address information field remains empty.

After receiving and validating the Activate PDP Context Request message by the SGSN, a corresponding Create PDP Context Request message (step 2) is sent from the SGSN to the affected GGSN 20. The GGSN 20 may use the included APN to find an external service or to activate a service for the APN.

Furthermore, an IPv6 address comprising an IPv6 prefix and an interface identifier is allocated for the UE 10 by the GGSN (steps 3 to 5). The GGSN 10 creates a new entry in a register comprising a corresponding PDP context table. The new entry allows the GGSN 10 to route PDP protocol data units (PDU) between the SGSN and an external PDP network.

Since the operator network 100 is IPv4 based, a transition mechanism according to ISATAP is also executed by the GGSN 20. Therefore, an ISATAP address is required for the UE 10. After allocating the IPv6 prefix, an ISATAP format interface identifier (i.e., an IPv4 address) should be assigned to the UE 10. However, as the UE 10 may choose to use a different interface identifier without involving the network (as specified, for example, in 3GPP TS 23.060), an allocation of such an ISATAP format interface identifier directly to the UE is not preferable. Instead, the GGSN 20 keeps the relationship between the PDP context (IPv6) and its corresponding IPv4 address (used for ISATAP) while the PDP context with the UE 10 is active. The GGSN 20 allocates also an IPv4 address, associates the IPv4 address with the

allocated PDP address, and stores (updates) this association in the corresponding entry of the GGSN's PDP context table by adding the information element, for example, in a 32-bit field to the table containing the IPv4 address. The 32-bit field can be defined, for example, as a "V4_ISATAP_ADDR" field. In the present embodiment, the GGSN 20 comprises a pool of (private) IPv4 addresses for the allocation. It is to be noted that due to the huge number of terminals in a 3GPP network and the lack of public IPv4 addresses, it is preferable to allocate private IPv4 addresses for ISATAP since public addresses are not necessary for the tunneling mechanism.

In other words, in the present embodiment, the standard procedure is followed to allocate an interface identifier for the UE, but when the GGSN 20 creates a new entry in the PDP context table to store the assigned IPv6 prefix, it allocates also an IPv4 address (ISATAP interface identifier) and stores this in the new entry of the PDP context table under the "V4_ISATAP_ADDR" field. The allocation of the IPv4 address by the GGSN 20 is performed by using a pool of IPv4 addresses maintained in the GGSN 20.

Then, the GGSN 20 returns a Create PDP Context Response message (step 6) to the SGSN including the PDP address allocated by the GGSN 20. The SGSN processes the information comprised in the response message (i.e. inserting PDP address received from the GGSN 20, selecting connection resources and the like) and sends a Activate PDP context Accept message to the UE 10 (step 7) for completing the establishment of the communication connection. The above described steps 6 and 7 can be equivalent to corresponding steps defined in 3GPP TS 23.060.

Next, a second embodiment is described with reference to Fig. 4. Those network elements and processing steps of this embodiment being equivalent to those of the first embodiment are not described in detail for simplification.

The present embodiment differs from the first embodiment with regard to the allocation process of the IPv4 and IPv6 addresses in the GGSN 20 (steps 3 to 5 in Fig. 4). In detail, according to the present embodiment, the GGSN 20 is configured, for example by the network operator, to use an external address allocation element for requesting a respective IP address. The usage of such an external address allocation element can be specified or decided in dependence on the APN indicated in the Activate PDP context Request message (step 1). The external address allocation element can be implemented, for example, by means of a Dynamic Host Control Protocol (DHCP) client (not shown) in the GGSN and a corresponding DHCP server (not shown) contacted by the DHCP client.

As illustrated in Fig. 4, after the SGSN has sent the Create PDP context Request message (step 2) to the GGSN 20, and the address allocation is indicated to be externally controlled (e.g. by evaluating the APN), the GGSN 20 initially sets the PDP address for the UE 10 to 0.0.0.0, and this address is returned to the UE 10 via the SGSN. This specific PDP address indicates that the PDP address shall be negotiated by the UE with the external packet data network after completion of the PDP Context Activation procedure. The GGSN is adapted to relay, modify and monitor these negotiations as long as the PDP context is in an ACTIVE state,.

Furthermore, with regard to the allocation of the IPv4 address for the ISATAP link, the GGSN 20 uses also an

external address allocation element. This means that the GGSN 20 implements the DHCP client and requests the IPv4 address from a DHCP server (not shown). Similar to the first embodiment, the GGSN 20 keeps the relationship between the PDP context (IPv6) and the corresponding IPv4 address (used for ISATAP) while the PDP context with the UE 10 is active. The GGSN 20 requests an IPv4 address from the external address allocation element, associates the received IPv4 address with the allocated PDP address, and stores (updates) this association in the corresponding entry of the GGSN's PDP context table by adding the information element, for example, in the 32-bit field "V4_ISATAP_ADDR" to the table containing the IPv4 address.

Thus, according to the proposed solution as described in the two embodiments above, it is possible to implement a transition mechanism such as ISATAP in communication networks, e.g. 3GPP based, in a manner which requires no specific changes in the user terminal nodes. This means, that IPv6-in-IPv4 tunneling is completely transparent to the (user) terminal nodes. This is achieved, for example, by defining an ISATAP proxy in the GGSN, which performs all the ISATAP node functionality on behalf of the corresponding UE. The proposed solution can be implemented as a software upgrade in the GGSN wherein a new field (e.g. "V4_ISATAP_ADDR") is added to the PDP context table, and the GGSN is capable of allocating or requesting (either from a pool of private IPv4 addresses or by using a DHCP client/server architecture) and storing a corresponding IPv4 address associated with an allocated IPv6 address. The so-called 6in4 tunneling is performed by the GGSN using the IPv4 address stored in the corresponding entry of the PDP context table.

In the above described first embodiment, the allocation of IPv6 addresses and IPv4 addresses is performed directly by the GGSN 20, while in the second embodiment the allocation of IPv6 addresses and IPv4 addresses is performed by using an external address allocation element such as a DHCP client/server architecture. However, it is also possible to combine these features in such that one type of the addresses is allocated by the GGSN while the other type of the addresses is allocated by the external address allocation element.

Moreover, even though the present invention is described in connection with the first and second embodiments related to the ISATAP based transition mechanism and the 3GPP based mobile communication network, it is to be understood that the application of the proposed solution is not limited to this scenario. For example, the presented solution can also be applied for other communication network types, for example, 3GPP2 based or fixed communication networks. Also the utilized transition mechanism can be of a different type. The proposed solution is in general applicable to any other automatic tunneling mechanism which requires tunneling (i.e. encapsulation/decapsulation) to be performed in the user terminal (UE). For example, the proposed solution could be implemented in connection with the so-called Teredo mechanism (UDP tunneling) proposed by C. Huitema et al., or the 6over4 mechanism proposed by B. Carpenter et al. (see also RFC 2529).

As described above, there is disclosed that a data transmission from a first node, such as a user equipment UE, to a second node, such as an application server or IMS, via a communication network using different types of communication protocols, such as a 3GPP communication network using IPv6 and IPv4, is controlled by means of a

transition mechanism, such as ISATAP. The transition mechanism is located in the communication network, for example, in a gateway node like a GGSN, which acts as a transition mechanism proxy. A data transmission from the first node is forwarded (or tunneled) by the network node to the second node wherein the transition mechanism functionality is performed in the network node transparently for the first node.

It should be understood that the above description and accompanying figures are merely intended to illustrate the present invention by way of example only. The described embodiments of the present invention may thus vary within the scope of the attached claims.

EPO - Munich
3
27. Juni 2003

CLAIMS

1. A method of controlling a data transmission from a first node to a second node via a communication network wherein the first node is connected to the communication network by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node,

the method comprising the steps of:

activating a communication connection based on the communication protocol of the first type from the first node to a network node of the communication network;

allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node;

allocating, based on a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node; and

storing, by the network node, the first connection information part and the second connection information part in a register, wherein the second connection information

part is associated with the first connection information part in a common entry in the register.

2. The method according to claim 1, wherein, in the step of activating the communication connection, an activation request is sent from the first node to the network node, the activation request comprising at least one of an indication for a dynamic addressing and an indication of an address type for the communication protocol of the first type.

3. The method according to claim 1 or 2, wherein, in the step of allocating the first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, the address related to the communication protocol of the first type is allocated by the network element.

4. The method according to claim 1 or 2, wherein, in the step of allocating the first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node, the address related to the communication protocol of the first type is requested from an external address allocation element contacted by the network element.

5. The method according to any of claims 1 to 4, wherein, in the step of allocating the second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, the address related to the communication protocol of the second type is allocated by the network element from an internal pool of addresses.

6. The method according to any of claims 1 to 4, wherein, in the step of allocating the second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node, the address related to the communication protocol of the second type is requested from an external address allocation element contacted by the network element.

7. The method according to any of the preceding claims, wherein, in the storing step, the network element stores the first connection information part and the second connection information part associated with each other by an entry in a table portion related to the communication connection of first node, wherein the second connection information part is stored in a specific table field of the table portion.

8. The method according to any of the preceding claims, further comprising a step of tunneling, via the network node, the data transmission based on the communication protocol of the first type between the first node and the second node by means of a connection based on the communication protocol of the second type.

9. The method according to any of the preceding claims, wherein the data transmission is a packet based data transmission, the communication protocol of the first type is one type of an Internet protocol, in particular an IPv6 based protocol, and the communication protocol of the second type is another type of an Internet protocol, in particular an IPv4 based protocol.

10. The method according to any of the preceding claims, wherein the communication connection between the first node and the network node is based on a packet based data

transmission protocol context, in particular on a Packet Data Protocol context.

11. The method according to any of the preceding claims, wherein the transition mechanism used by the communication network is an automatic tunneling mechanism which uses in particular the Intra-Site Automatic Tunnel Addressing Protocol.

12. The method according to any of the preceding claims, wherein the network node is a gateway node of the communication network, in particular a Gateway GPRS Support Node.

13. A system for controlling a data transmission from a first node to a second node via a communication network wherein the first node is connected to the communication network by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node,

the system comprising:

means for activating a communication connection based on the communication protocol of the first type between the first node and a network node of the communication network;

means for allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node;

means for allocating, on the basis of a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node; and

means for associating the second connection information part with the first connection information part

and for storing the associated first and second connection information parts in a register.

14. The system according to claim 13, wherein the means for activating the communication connection comprises means for sending and receiving an activation request from the first node to the network node, the activation request comprising at least one of an indication for a dynamic addressing and an indication of an address type for the communication protocol of the first type.

15. The system according to claim 13 or 14, wherein the means for allocating the first connection information part is part of the network node wherein the address related to the communication protocol of the first type is allocated by the network element.

16. The system according to claim 13 or 14, wherein the means for allocating the first connection information part is part of the network node wherein the address related to the communication protocol of the first type is requested from an external address allocation element contacted by the network element.

17. The system according to any of claims 13 to 16, wherein the means for allocating the second connection information part is part of the network node wherein the address related to the communication protocol of the second type is allocated by the network element and selected from an internal pool of addresses.

18. The system according to any of claims 13 to 16, wherein the means for allocating the second connection information part is part of the network node wherein the address related to the communication protocol of the second type is

requested from an external address allocation element contacted by the network element.

19. The system according to any of claims 13 to 18, wherein the means for storing stores the associated first and second connection information parts in a register of the network element by updating an entry in a table portion related to the communication connection of first node, wherein the second connection information part is stored in a specific table field of the table portion.

20. The system according to any of claims 13 to 19, wherein the data transmission based on the communication protocol of the first type is tunneled between the first node and the second node by the network node by means of a connection based on the communication protocol of the second type.

21. The system according to any of claims 13 to 20, wherein the data transmission is a packet based data transmission, the communication protocol of the first type is one type of an Internet protocol, in particular an IPv6 based protocol, and the communication protocol of the second type is another type of an Internet protocol, in particular an IPv4 based protocol.

22. The system according to any of claims 13 to 21, wherein the communication connection between the first node and the network node is based on a packet based data transmission protocol context, in particular on a Packet Data Protocol context.

23. The system according to any of claims 13 to 22, wherein the transition mechanism used by the communication network is an automatic tunneling mechanism which uses in

particular the Intra-Site Automatic Tunnel Addressing Protocol.

24. The system according to any of claims 13 to 23, wherein the network node is a gateway node of the communication network, in particular a Gateway GPRS Support Node.

25. A network node of a communication network, the network node being usable for controlling a data transmission from a first node to a second node via the communication network wherein the first node is connected to the network node by means of a communication protocol of a first type and the communication network uses at least in part a communication protocol of a second type for forwarding the data transmission from the first node to the second node,

the network node comprising:

means for activating a communication connection based on the communication protocol of the first type between the first node and the network node;

means for allocating a first connection information part comprising an address related to the communication protocol of the first type to the communication connection of the first node;

means for allocating, on the basis of a transition mechanism used by the communication network, a second connection information part comprising an address related to the communication protocol of the second type to the communication connection of the first node; and

means for associating the second connection information part with the first connection information part and for storing the associated first and second connection information parts in a register.

26. The network node according to claim 25, wherein the means for activating the communication connection comprises means for receiving an activation request from the first

node, the activation request comprising at least one of an indication for a dynamic addressing and an indication of an address type for the communication protocol of the first type.

27. The network node according to claim 25 or 26, wherein the means for allocating the first connection information part comprises addresses related to the communication protocol of the first type and allocates a selected one of the addresses.

28. The network node according to claim 25 or 26, wherein the means for allocating the first connection information part requests an address for the address related to the communication protocol of the first type from an external address allocation element.

29. The network node according to any of claims 25 to 28, wherein the means for allocating the second connection information part comprises a pool of addresses related to the communication protocol of the second type and allocates a selected one of the addresses.

30. The network node according to any of claims 25 to 28, wherein the means for allocating the second connection information part requests an address for the address related to the communication protocol of the second type from an external address allocation element.

31. The network element according to any of claims 25 to 30, wherein the means for storing stores the associated first and second connection information parts in a register of the network element by updating an entry in a table portion related to the communication connection of first node, wherein the second connection information part is stored in a specific table field of the table portion.

32. The network node according to any of claims 25 to 31, wherein the network nodes tunnels the data transmission based on the communication protocol of the first type between the first node and the second node by means of a connection based on the communication protocol of the second type.

33. The network node according to any of claims 25 to 32, wherein the data transmission is a packet based data transmission, the communication protocol of the first type is one type of an Internet protocol, in particular an IPv6 based protocol, and the communication protocol of the second type is another type of an Internet protocol, in particular an IPv4 based protocol.

34. The network node according to any of claims 25 to 33, wherein the communication connection between the first node and the network node is based on a packet based data transmission protocol context, in particular on a Packet Data Protocol context.

35. The network node according to any of claims 25 to 34, wherein the transition mechanism used by the communication network is an automatic tunneling mechanism which uses in particular the Intra-Site Automatic Tunnel Addressing Protocol.

36. The network node according to any of claims 25 to 35, wherein the network node is a gateway node of the communication network, in particular a Gateway GPRS Support Node.

EPO - Munich
3
27. Juni 2003

ABSTRACT
(FIG. 1)

A data transmission from a first node, such as a user equipment UE, to a second node, such as an application server or IMS, via a communication network using different types of communication protocols, such as a 3GPP communication network using IPv6 and IPv4, is controlled by means of a transition mechanism, such as ISATAP. The transition mechanism is located in the communication network, for example, in a gateway node like a GGSN, which acts as a transition mechanism proxy. A data transmission from the first node is forwarded (or tunneled) by the network node to the second node wherein the transition mechanism functionality is performed in the network node transparently for the first node.

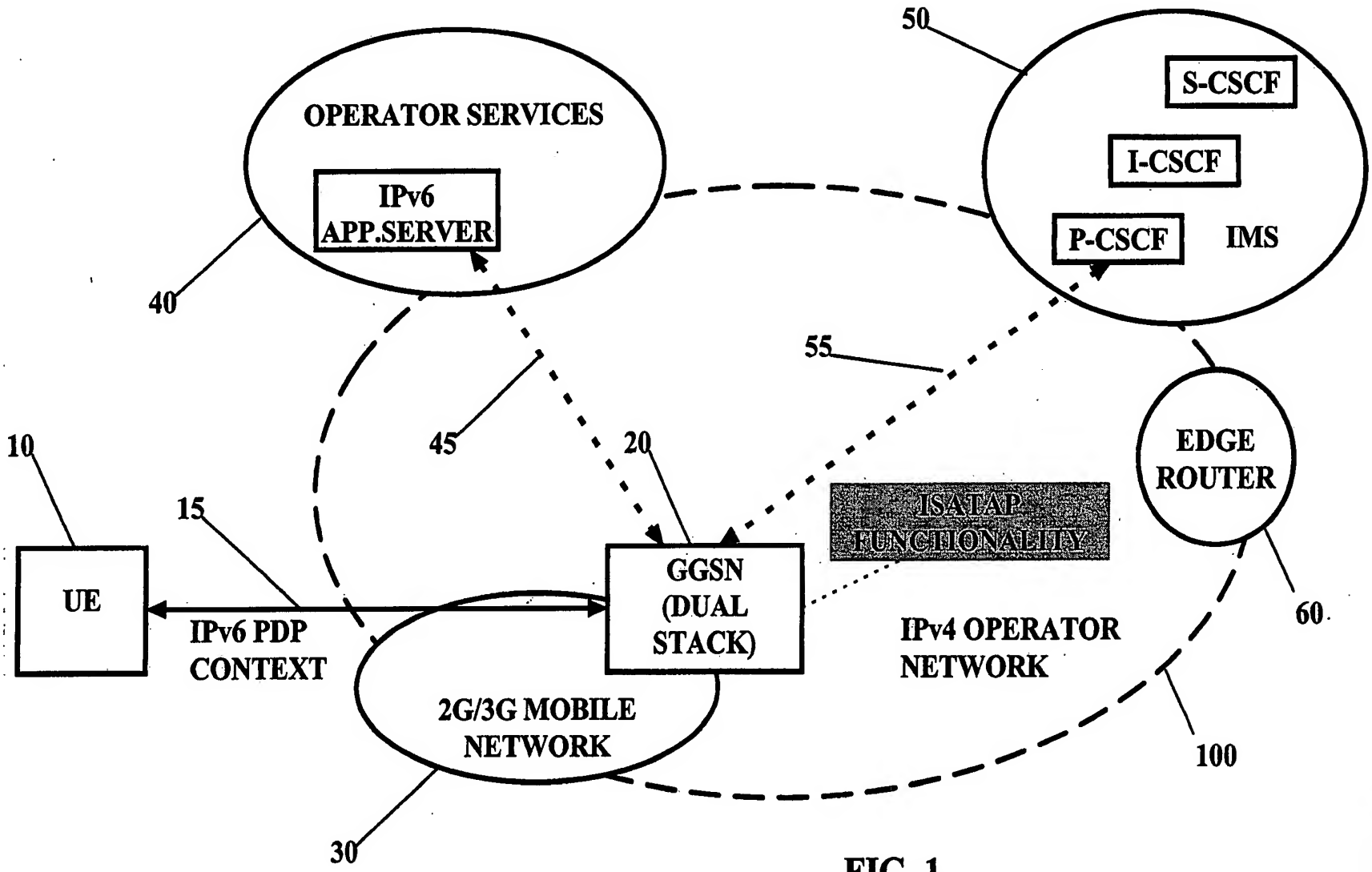


FIG. 1

EPO - Munich
3
27. Juni 2003

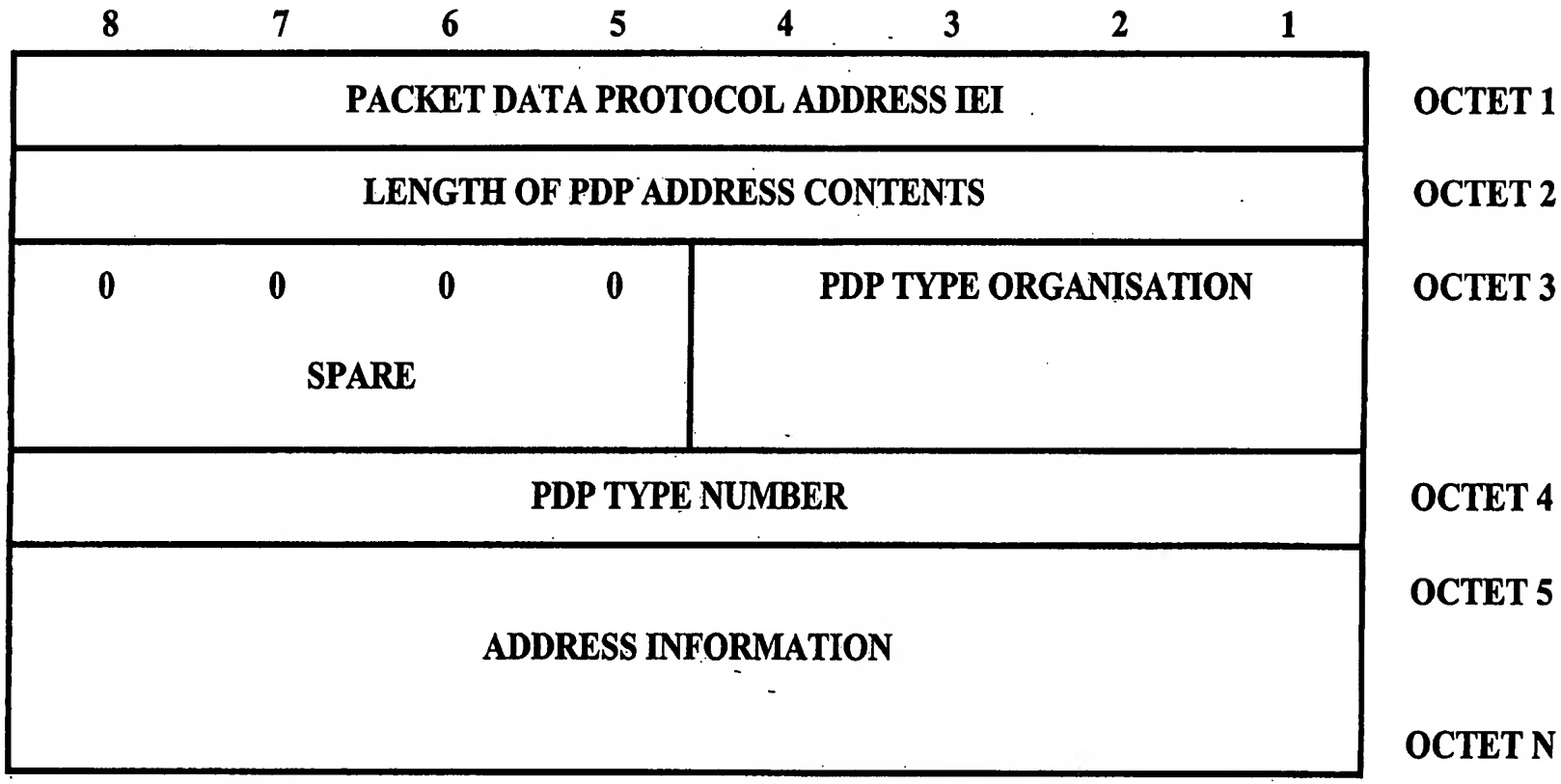

8 7 6 5 4 3 2 1
PACKET DATA PROTOCOL ADDRESS IEI
OCTET 1
LENGTH OF PDP ADDRESS CONTENTS
OCTET 2
0 0 0 0
SPARE
PDP TYPE ORGANISATION
OCTET 3
PDP TYPE NUMBER
OCTET 4
ADDRESS INFORMATION
OCTET 5
OCTET N

FIG. 2

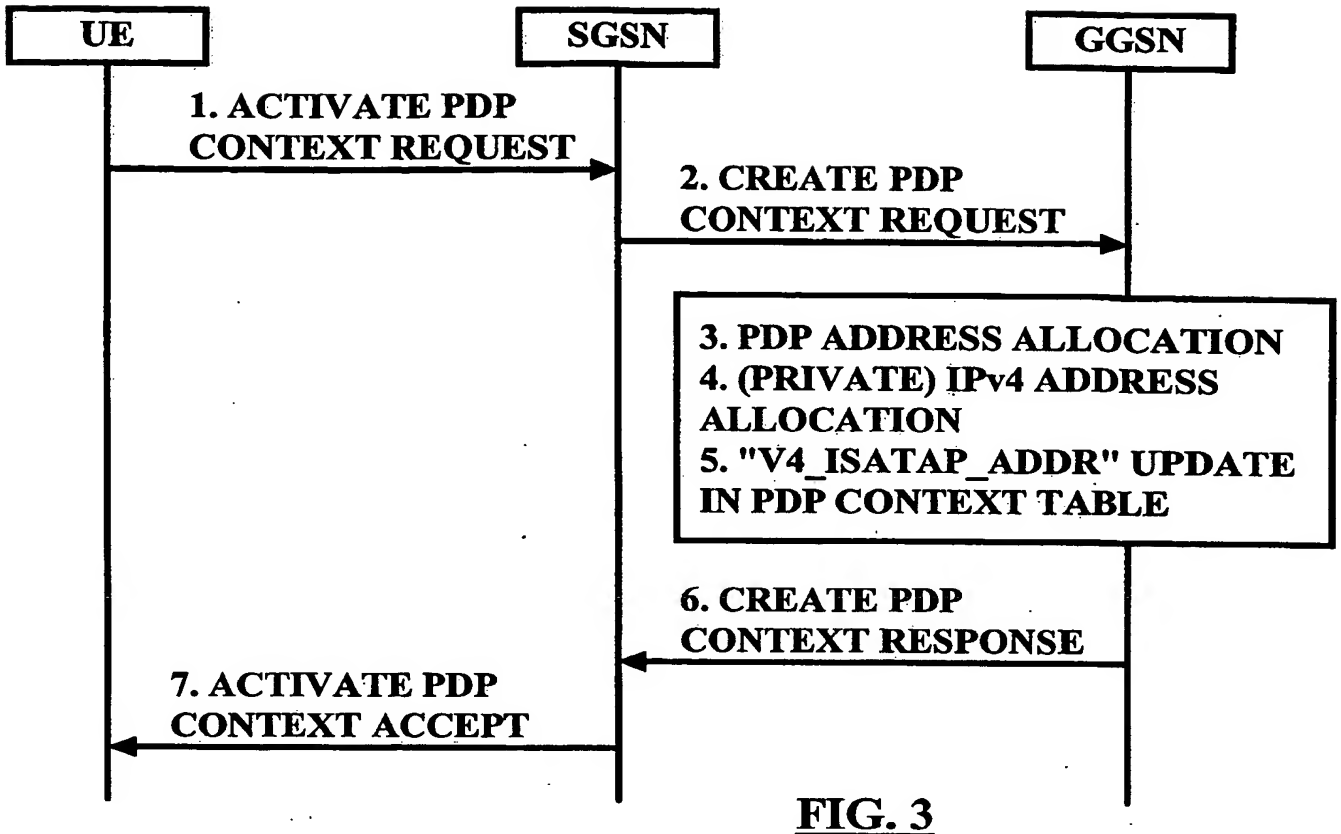

UE
SGSN
GGSN
1. ACTIVATE PDP CONTEXT REQUEST
2. CREATE PDP CONTEXT REQUEST
3. PDP ADDRESS ALLOCATION
4. (PRIVATE) IPv4 ADDRESS ALLOCATION
5. "V4_ISATAP_ADDR" UPDATE IN PDP CONTEXT TABLE
6. CREATE PDP CONTEXT RESPONSE
7. ACTIVATE PDP CONTEXT ACCEPT

FIG. 3

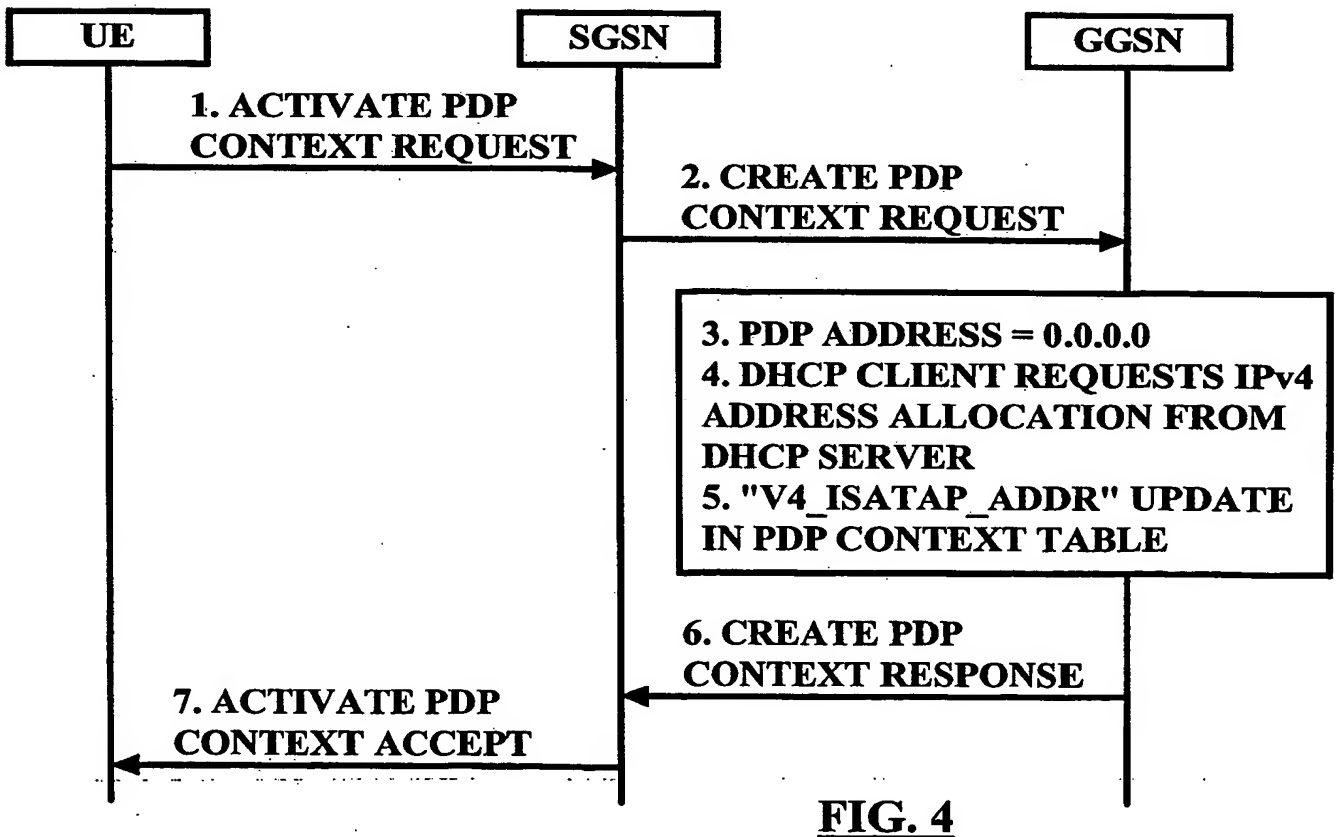

UE
SGSN
GGSN
1. ACTIVATE PDP CONTEXT REQUEST
2. CREATE PDP CONTEXT REQUEST
3. PDP ADDRESS = 0.0.0.0
4. DHCP CLIENT REQUESTS IPv4 ADDRESS ALLOCATION FROM DHCP SERVER
5. "V4_ISATAP_ADDR" UPDATE IN PDP CONTEXT TABLE
6. CREATE PDP CONTEXT RESPONSE
7. ACTIVATE PDP CONTEXT ACCEPT

FIG. 4

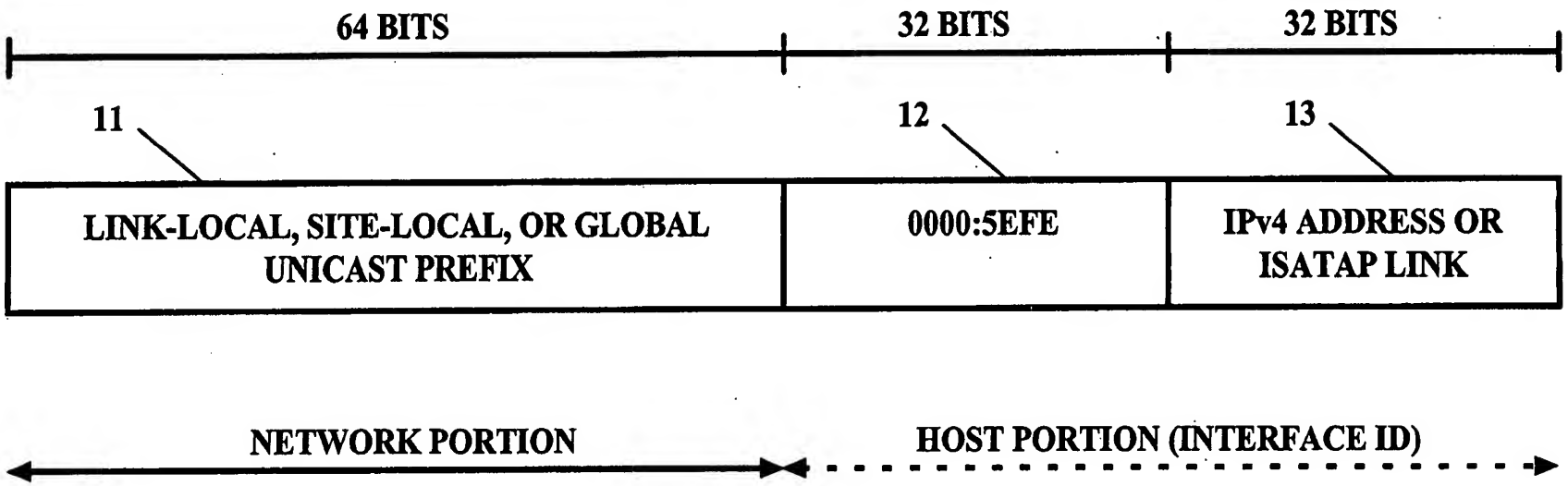

64 BITS
32 BITS
32 BITS
11
12
13
LINK-LOCAL, SITE-LOCAL, OR GLOBAL UNICAST PREFIX
0000:5EFE
IPv4 ADDRESS OR ISATAP LINK
NETWORK PORTION
HOST PORTION (INTERFACE ID)

FIG. 5

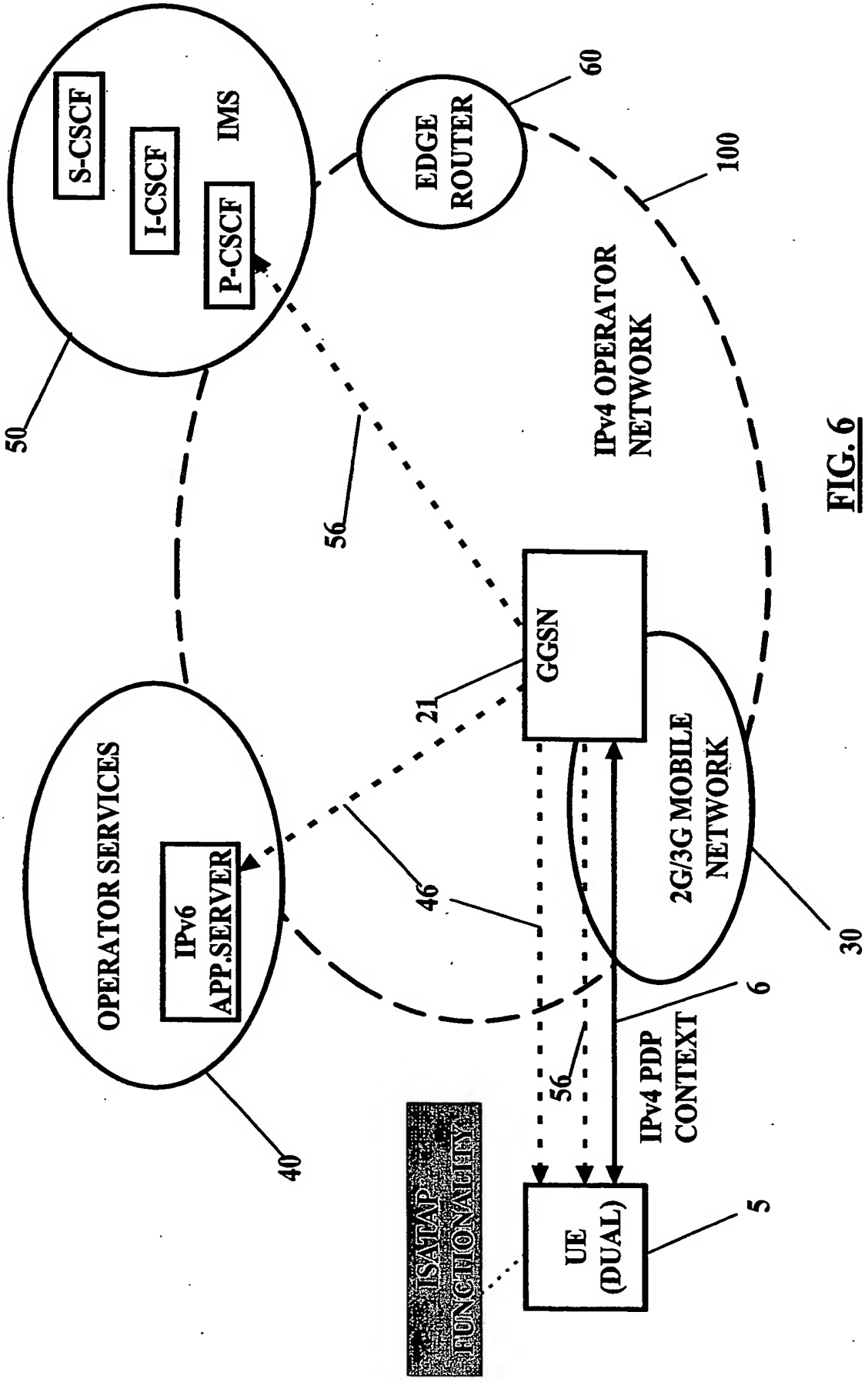

S-CSCF
I-CSCF
P-CSCF
IMS
50
EDGE ROUTER
60
100
IPv4 OPERATOR NETWORK
56
GGSN
21
OPERATOR SERVICES
IPv6 APP.SERVER
40
46
2G/3G MOBILE NETWORK
30
6
IPv4 PDP CONTEXT
56
ISATAP FUNCTIONALITY
UE (DUAL)
5

FIG. 6